

# 네트워크 공격 방지를 지원하는 DHCP에 관한 연구

김문기\*, 정다혜\*, 이재원\*, 유권정\*, 김은기\*

\*한밭대학교 정보통신공학과

e-mail : kmg8498@naver.com

## A Study on the DHCP Supporting Network Attack Prevention

Moon-Gi Kim\*, Da-Hye Jeong\*, Jae-Won Lee\*, Kwon-Jeong Yoo\*, Eun-Gi Kim\*

\*Dept. of Information and Communication Engineering, Han-Bat University

### 요약

DHCP(Dynamic Host Configuration Protocol)는 TCP/IP 통신을 실행하기 위해 필요한 IP 주소 및 관련된 세부 구성 정보를 자동적으로 할당한다. 기존의 DHCP는 서버와 클라이언트 간 상호 인증 체계가 없어서 다양한 네트워크 공격에 취약하다. 본 논문에서는 기존 DHCP 메시지 옵션에 네트워크 공격을 방지할 수 있도록 지원하는 옵션을 추가하였다. DHCP 통신 과정에서 ECDSA와 HMAC 알고리즘 등을 이용하여 메시지의 무결성을 보장하고 서버와 클라이언트 간 상호 인증을 수행한다.

### 1. 서론

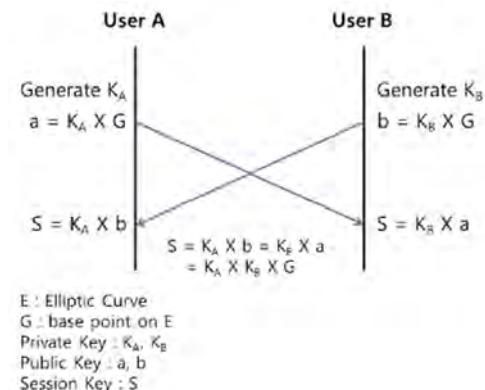
DHCP(Dynamic Host Configuration Protocol)는 표준 TCP/IP 호스트 설정 프로토콜이며 하나의 클라이언트만을 포함하는 홈 네트워크부터 회사 수준의 인터넷워크에 이르기까지 모든 부문에서 사용된다[1].

DHCP는 넓은 사용 범위에 따라 DHCP release attack, rogue DHCP attack 등 다양한 네트워크 공격에 노출되어 있다. 이러한 이유로 본 논문에서는 안전하게 DHCP를 사용하기 위해서 ECDH(Elliptic Curve Diffie-Hellman), ECDSA(Elliptic Curve Digital Signature Algorithm), HMA-C(Hash-based Message Authentication Code)을 이용하여 DHCP 메시지의 옵션을 추가하였다. 본 논문의 구성은 다음과 같다. 2 장에서는 ECDH 키 교환 알고리즘, ECDSA, HMAC에 대하여 설명한다. 3 장에서는 DHCP 메시지 옵션의 설계에 대하여 기술하고, 4 장에서는 결론을 다룬다.

### 2. 관련 연구

#### 2.1. ECDH 키 교환 알고리즘

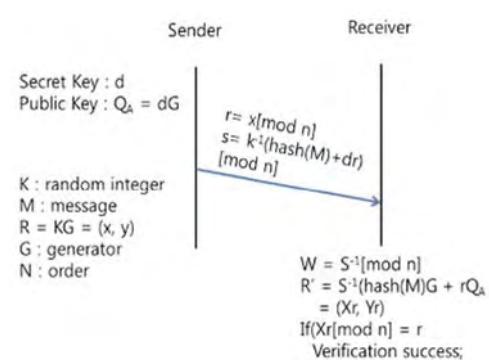
ECDH는 DH(Diffie-Hellman) 키 교환 알고리즘에 ECC(Elliptic Curve cryptography) 방식을 적용한 키 교환 알고리즘이다. ECC 방식을 사용하면 기존의 알고리즘과 같은 정도의 안전성을 보장한다고 했을 때 키의 길이가 짧은 이점이 있다[2]. (그림 1)은 ECDH 키 교환 알고리즘을 이용하여 세션 키를 생성하는 과정을 나타낸다.



(그림 1) ECDH를 이용한 세션 키 생성 과정

#### 2.2. ECDSA

ECDSA는 DSA(Digital Signature Algorithm)에 ECC 방식을 적용한 알고리즘이다. (그림 2)는 송신자가 ECDSA를 이용하여 전자 서명을 생성하고, 수신자가 전자 서명을 검증하는 과정을 나타낸다.

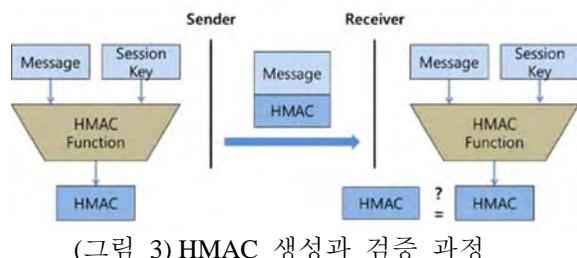


(그림 2) ECDSA를 이용한 전자 서명 생성과 검증 과정

### 2.3. HMAC

HMAC 은 사용자의 비밀 키와 메시지를 해시 함수에 입력하여 해시 코드를 생성하는 방법으로 데이터의 무결성을 보장한다. 본 논문에서는 ECDH 에서 얻은 세션 키를 해시함수의 입력에 사용되는 비밀 키로 사용한다.

송신자는 HMAC 함수 입력 값으로 메시지와 세션 키를 사용하여 HMAC 을 생성한다. 송신자는 메시지 뒤에 HMAC 을 추가하여 수신자에게 전송한다. 수신자는 수신한 메시지와 세션 키를 비교하여 HMAC 을 생성하고 수신한 HMAC 과 비교하여 메시지의 무결성을 검증한다. (그림 3)은 HMAC 함수를 이용하여 HMAC 을 생성하고, 검증하는 과정을 나타낸다.



(그림 3) HMAC 생성과 검증 과정

### 3. DHCP 메시지 옵션의 설계

본 논문에서 제안하는 DHCP 메시지 옵션의 설계는 2 장의 연구들을 바탕으로 한다.

#### 3.1. 메시지 옵션의 형식

옵션 코드(Code)는 할당되어 있지 않은 번호인 222 를 사용한다[3]. (그림 4)는 DHCP 메시지 옵션의 형식을 나타낸다.

Code	Length	Algorithm	Authentication Information
------	--------	-----------	----------------------------

(그림 4) DHCP 메시지 옵션의 형식

길이 필드(Length)는 알고리즘 필드(Algorithm)와 인증 정보 필드(Authentication Information)의 데이터 길이를 Octets 으로 표기한다. 알고리즘 필드는 ECDH 키 길이와 HMAC 종류를 명시한다. 인증 정보 필드는 ECDH 공개 키, HMAC, nonce, ECDSA 로 이루어진다. 또한 인증 정보 필드는 메시지의 종류에 따라 선택적으로 사용된다.

#### 3.2. 제안하는 옵션의 동작

##### 3.2.1. 알고리즘 협상

클라이언트는 IP 주소를 할당 받기 위해서 서버에게 DHCPDISCOVER 메시지를 전송한다. 메시지의 알고리즘 필드는 클라이언트가 지원 가능한 ECDH 키 길이와 HMAC 종류로 구성된다.

DHCPDISCOVER 메시지를 수신한 서버는 DHCPOFFER 메시지를 클라이언트에게 전송한다. 서버는 클라이언트가 요청한 알고리즘 중에서 사용할 알고리

즘을 선택하고, 메시지의 인증 정보 필드에 nonce 와 전자 서명을 포함시킨다.

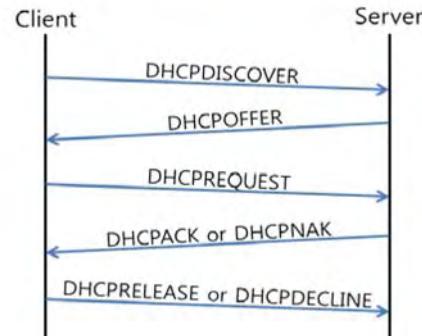
##### 3.2.2. ECDH 키 교환 과정

클라이언트가 DHCPOFFER 메시지를 수신하면 서버에게 DHCPREQUEST 메시지를 전송한다. 메시지의 인증 정보 필드는 서버가 선택한 알고리즘 종류로 생성한 ECDH 공개 키로 구성된다.

서버가 DHCPREQUEST 메시지를 수신하면 DHCPACK 또는 DHCPNAK 메시지로 응답한다. 서버가 DHCPACK 메시지를 전송하는 경우, 메시지의 인증 정보 필드에 서버의 공개 키, nonce, 전자 서명을 포함시킨다. 서버가 DHCPNAK 메시지를 전송하는 경우, 메시지의 인증 정보 필드에 nonce 와 전자 서명을 포함시킨다.

클라이언트가 DHCPACK 메시지를 수신하는 경우, 서버로부터 임대 받은 주소를 검사한다. 주소가 이미 사용 중이면 DHCPDECLINE 메시지를 전송한다. 메시지의 인증 정보 필드에 세션 키를 이용하여 생성한 HMAC 을 포함한다. 주소가 사용 중이지 않으면 할당 과정을 완료한다.

클라이언트가 IP 주소의 사용을 마치는 경우, DHCPRELEASE 메시지를 전송한다. 이때 메시지의 인증 정보 필드는 세션 키를 이용하여 만든 HMAC 을 포함한다. (그림 5)는 할당 과정 또는 재할당 과정에서 송수신 하는 메시지를 나타낸다.



(그림 5) 할당 과정 또는 재할당 과정에서 송수신 하는 메시지

##### 3.2.3. 임대 갱신 과정

클라이언트는 할당 또는 재할당 과정이 완료될 때 두 개의 타이머를 설정한다. 일반적으로 갱신 타이머는 임대 기간의 50%, 리바인딩 타이머는 임대 기간의 87.5%로 설정한다.

클라이언트는 갱신 타이머가 만료되면 임대의 연장과 새로운 세션 키를 갱신하기 위해서 DHCPREQUEST 갱신 메시지를 전송한다. DHCPREQUEST 갱신 메시지는 클라이언트의 새로운 공개 키와 안전하게 키를 교환하게 위해서 이전의 세션 키로 생성한 HMAC 을 포함한다.

서버가 DHCPREQUEST 갱신 메시지를 수신하면 DHCPACK 또는 DHCPNAK 메시지를 클라이언트에게

전송한다. 서버가 DHCPACK 메시지를 전송하는 경우, 서버의 새로운 ECDH 공개 키, nonce, 전자 서명을 포함하고, DHCPNAK 메시지를 전송하는 경우에는 nonce, 전자 서명을 포함시킨다.

#### 4. 결론

본 논문에서는 다양한 네트워크 공격을 방지하기 위해 DHCP 임대 과정에서 서버와 클라이언트의 상호 인증을 수행하고, 메시지의 무결성을 보장하는 DHCP 메시지 옵션을 제안하였다.

서버는 ECDSA를 이용하여 생성한 전자 서명을 서버가 전송하는 모든 메시지에 포함하여 정상적인 서버임을 인증하고 메시지의 무결성을 보장한다.

서버와 클라이언트는 ECDH 키 교환 알고리즘을 이용하여 공통의 세션 키를 생성한다. 키 교환이 완료된 이후 클라이언트는 전송하는 메시지에 세션 키로 생성한 HMAC을 포함하여 클라이언트의 인증과 메시지의 무결성을 보장한다.

#### 감사의 글

본 연구는 중소기업청에서 지원하는 2015년도 이공계 전문가 기술개발 서포터즈 사업(No. C03439530100434374)의 연구수행으로 인한 결과물임을 밝힙니다.

#### 참고문헌

- [1] Charles M. Kozierok, “TCP/IP 완벽 가이드”, 에이콘 출판주식회사, 2007.
- [2] 칼리스 아담스, 스티브 로이드 공저, 장기식 역, “보안을 위한 효율적인 방법 PKI”, 인포북, 2003
- [3] S. Alexander, R. Droms, “DHCP Options and BOOTP Vendor Extensions”, RFC 2132, IETF, March 1997
- [4] R. Droms, “Dynamic Host Configuration Protocol”, RFC 2131, IETF, March 1997
- [5] R. Droms, W. Arbaugh, “Authentication for DHCP messages”, RFC 3118, IETF, June 2001
- [6] Behrouz A. Forouzan, “TCP/IP Protocol Suite, Fourth Edition”, McGRAW HILL INTERNATIONAL EDITION, 2010
- [7] S. Jiang, S. Krishnan, T. Mrugalski, “Privacy considerations for DHCP”, draft-ietf-dhc-dhcp-privacy-00, IETF, February 2015
- [8] D. Miles, W. Dec, J. Bristow, R. Maglione, “Forcerenew Nonce Authentication”, RFC6704, IETF, August 2012
- [9] T. Pornin, “Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)”, RFC 6979, IETF, August 2013
- [10] H. Krawczyk, M. Bellare, R. Canetti, “HMAC: Keyed-Hashing for Message Authentication”, RFC 2104, IETF, February 1997